ASP Privacy & Security Policies

Access

How does your system ensure that only authorized users have access to only minimum necessary information?

Permissions to access each area of the eClinicalWorks application are granted (or restricted) within the Systems Administration area of the application per CCHIT 2011 security requirements. Permissions are user and role-based; each user requires a user name and password. The system has lock-out features and audit logs are maintained of system activity. With regards to the SaaS hosting environment, access to the customer data repository is restricted to eClinicalWorks database personnel who are granted the minimum level of access to perform their daily functions. Database security restricts access to authorized users only.

Authorization

How does your system authorize users to access information?

The eClinicalWorks application supports user name/password strength rules to prevent unauthorized access to PHI. With regards to the hosting environment, eClinicalWeb will provide to Client a user name, password and other information required to use the Hosted application, upon written request from Client to eClinicalWeb. eClinicalWeb shall take reasonable measures to prevent unauthorized access and use the same security measures it uses to protect its own proprietary information. Client shall be solely responsible for the security of its passwords.

Authentication

How does your system ensure that the person accessing the system is who they say they are?

The application authentication capabilities include user name and password or fingerprint scan for two factor authentication. eClinicalWorks authenticates users before any access to PHI is allowed by X509 certificates. Regarding the SaaS hosting environment, use of the user name and password supplied to the Client by eClinicalWeb shall be authenticated against the Active Directory maintained by eClinicalWeb.

Audit

What audit procedures are in place that will promote transparency and compliance with access, use, and disclosure requirements?

All transactions within the eClinicalWorks application are logged; the System Administrator has access to the entire system log-on record; all views, adds/deletes/modifications to a patient record are logged and are accessible in real-time from within the system. With regards to the SaaS hosting environment, eClinicalWeb shall monitor the System electronically in order to operate its System properly and to protect itself. Audit capabilities include the ability to identify who has accessed the System with full detail information and who has attempted access.

Secondary Uses of Data

How does your system ensure that the use and disclosure of information is limited to appropriate and approved users?

eClinicalWorks does not disclose any information as the data is owned by the client. Access is granted to certain eClinicalWorks personnel for customer service and system performance only. eClinicalWorks has security guidelines in place to restrict access to only those authorized to perform these functions.

Data Ownership

Where is the data stored and who owns the data?

With regards to a SaaS hosting environment, eClinicalWeb acknowledges and agrees that the data and information that is compiled or generated through the databases that are part of the Applications and that specifically relates to patients, patient care or physicians procedures or diagnosis and all right, title and interest therein, is and shall remain the exclusive property of the Client.

Sensitive Protected Health Information

Sensitive health information refers to select protected health information (PHI). Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of PHI that may be considered particularly private or sensitive to a patient such as genetic information, psychotherapy notes, substance abuse treatment records, etc.

A practice may choose to further restrict access to a patient's chart by utilizing the Patient Security Access Code (PSAC) setting. Practices can create confidential charts and/or Progress Notes for specific visits or occurrences. eClinicalWorks can be configured to allow access to a patient's record only to authorized providers/users who have specifically been granted permission to access the chart or encounter. In addition, the system can alert a provider that an assessment is flagged to enable confidential charting.

Yes	No	
✓	☐	*Does your system have the ability to identify PHI that is sensitive?*

If yes, explain: eClinicalWorks has several ways in which the patient chart (all of portions thereof) can be restricted. Patient Security Access Control (PSAC) can be enabled to provide additional security to the patient record and/or Progress Note. Using the PSAC setting, practices can configure diagnoses such as HIV, mental illness, etc to be accessible only to authorized users, creating a confidential chart.

Yes	No	
✓	☐	*Does your system have the ability to prohibit sensitive PHI from being shared electronically?*

If yes, explain: As stated above, a practice may choose to further restrict access to a patient's chart by utilizing the Patient Security Access Code (PSAC) setting. Practices can create confidential charts and/or Progress Notes for specific visits or occurrences. eClinicalWorks can be configured to allow access to a patient's record only to authorized providers/users who have specifically been granted permission to access the chart or encounter.

Yes	No	
✓	☐	*Does your system have the ability to break the glass (Break the glass refers to the ability to obtain health information in emergency situations where consumer consent has not been granted)?*

If yes, explain: In the event an unauthorized provider needs immediate access to a confidential note, a "Break the Glass" feature can be enabled. An audit log of "break the glass" activity is generated and includes user name, patient ID number, encounter date/time, access time stamp, reason for access, status and IP address of accessing user.

Consumer Accounting of Disclosures

How does your system generate reports for consumer of access to their records?

eClinicalWorks is compliant with the Accounting of Disclosures requirement outlined in Part 170.20(d) (Health Information Technology Standards) of federal regulations and has met NIST certification testing for 2011. The date, time, patient identification, user identification, and a description of the disclosure is recorded for disclosures for treatment, payment, and health care operations within the electronic health record.

Secondary Data Use

Does your EHR system have provisions which allow the EHR vendor to extract a Limited Data Set of patient information to use for research purposes by the EHR vendor or a third party, if the practice agrees to participate in a study?

eClinicalWorks does not disclose any information as the data is owned by the client. Access is granted to certain eClinicalWorks personnel for customer service and system performance only. eClinicalWorks has security guidelines in place to restrict access to only those authorized to perform these functions.